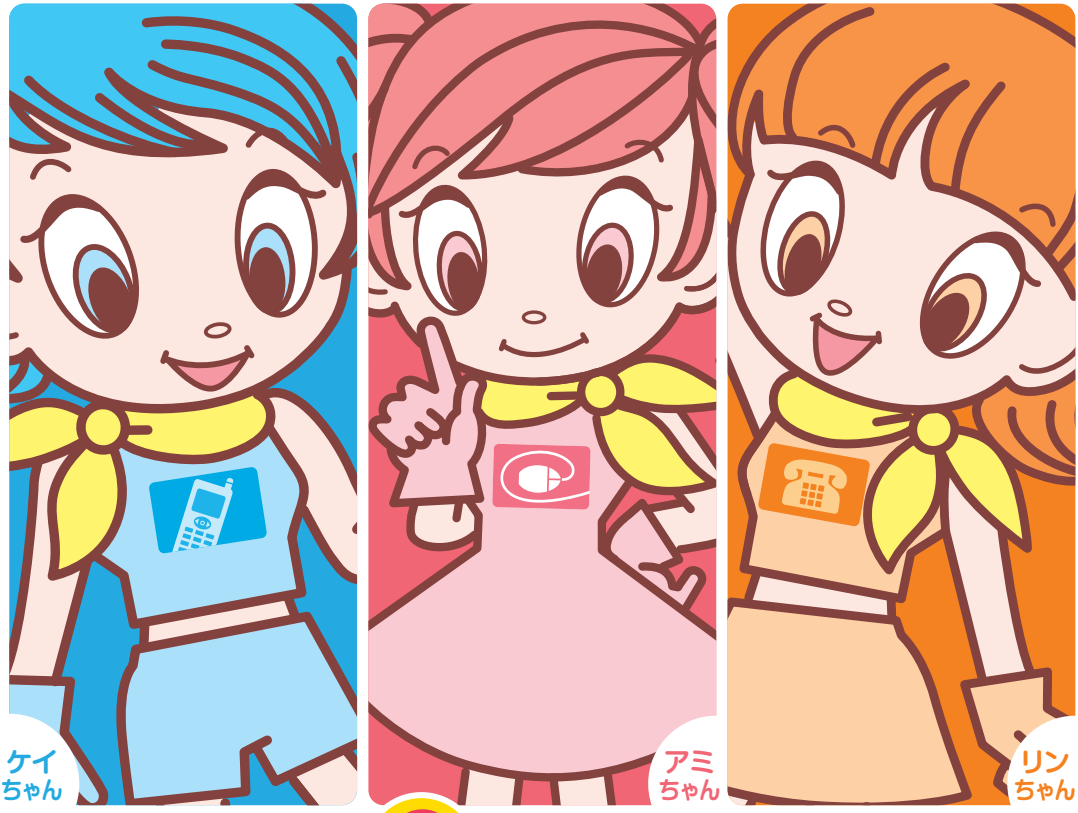
保存版　平成27年度

総務省

電気通信サービス Q&A

いざ!という時のお役立ち本



皆さんの？に私たちが答えます

いろんな「困った」に答えます
スマートフォン 携帯電話

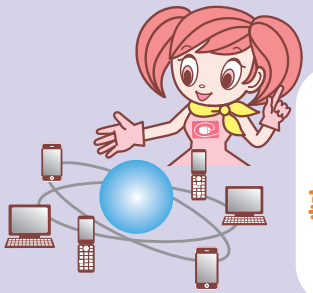
「セキュリティ」はしっかりと
インターネット

知っていますか?「災害時のサービス」
電話サービス

電気通信サービス Q&A

はじめに

国内電話、国際電話、インターネット、
スマートフォン、携帯電話…
電気通信サービスの発達によって、
わたしたちの生活は
かなり便利になりました。

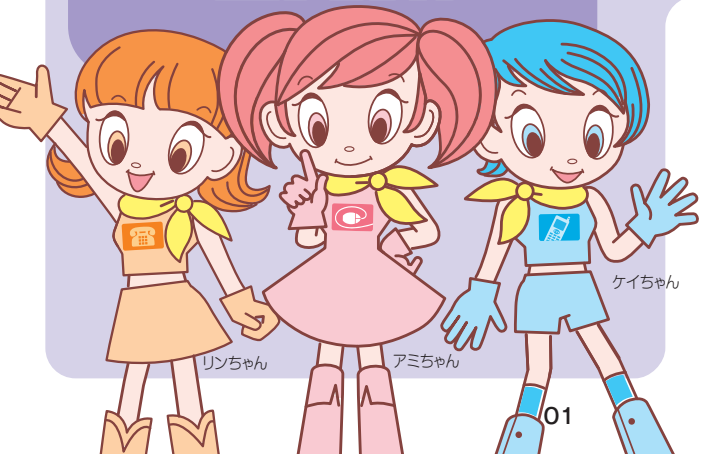


その一方で利用者の皆さんが
トラブルに巻き込まれる
ことも少なくありません。

そこで、電話やインターネットを
安心して利用するために、
事前のちょっとした知識
をご紹介します。

わたしたち「E-NAVIフレンズ」が
みなさんの「？」に
Q&A方式でわかりやすく
お答えします。
不安になったり、困った時はいつでも
お役立てください。

E-NAVIフレンズ



※電気通信サービスって?
電気通信を利用して提供されるサービスのことをいい、国内電話、国際電話、携帯電話、PHS、インターネット、FTTH等が対象になります。

文中に出てくる2つのマークに注目!

基礎知識 知っておきましょう … 利用するために知っておきたい基礎知識です。

注意 注意しましょう … トラブルになる可能性があるので十分に注意しましょう。

特集 スマートフォンの便利さと注意点 ……03
特集 ソーシャルメディアの利用の注意 ……06
特集 SIMロック解除、格安スマホについて ……07

知っ得情報

［知っ得情報］ トラブル防止のためのポイント Q&A
●勧誘や契約時の説明等に関するQ&A ……08
●架空請求・不当請求トラブルに関するQ&A ……13
●携帯電話やスマートフォンの高額パケット請求に関するQ&A ……15

携帯電話 スマートフォン

携帯電話・スマートフォンを快適に利用するために
●携帯電話利用時の注意点に関するQ&A ……16
●迷惑メールに関するQ&A ……19
●フィルタリングに関するQ&A ……22
●携帯電話とPHSの電話番号に関するQ&A ……25
●携帯電話・PHSの番号ポータビリティに関するQ&A ……26
●携帯電話不正利用防止法に関するQ&A ……27

インターネット

インターネットを楽しむために
●インターネット上の違法・有害情報に関するQ&A ……28
●フィッシング詐欺に関するQ&A ……30
●ネットセキュリティに関するQ&A ……31
●インターネット上のマナーに関するQ&A ……33

電話サービス

電話サービスをいつも安心・便利に利用するために
●災害時・停電時の電話サービスの利用に関するQ&A ……34
●災害用の伝言サービスに関するQ&A ……35
●ユニバーサルサービス制度に関するQ&A ……37

窓口一覧 ……38

特集

スマートフォンの便利さと注意点

Q01 これまでの携帯電話となにが違うの?

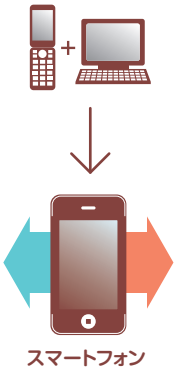
A01 基礎知識 知っておきましょう

スマートフォンは、**パソコンに近い**性質を持った携帯電話です。

便利さ

インターネット
パソコン用のウェブサイトの閲覧ができ、多様な情報収集が可能となります。

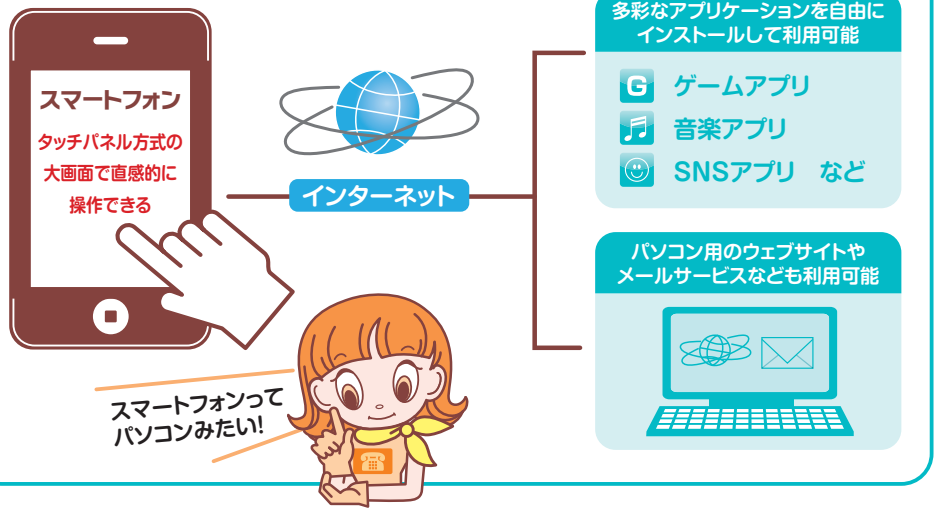
アプリケーション
多種多様なアプリケーション(アプリ)をインターネット上にあるサイト(マーケット)から利用者自身が自由に選択してダウンロードすることで、利用者が自ら端末をカスタマイズすることができ、利用者自身のニーズに合った便利な使い方が可能となります。



注意点

料金が高額になる危険性
パソコン用のウェブサイト閲覧や動画視聴をすると大容量のデータ通信が行われます。また、スマートフォンのアプリケーションには、自動的に通信を行うものもあります。

情報セキュリティ上の危険性
携帯電話事業者が管理するネットワークで提供するインターネット接続サービス(iモード、EZweb、Yahoo!ケータイ)を介さずにインターネットに接続することが可能となるため、従来の携帯電話端末と比較して情報セキュリティ上の危険性があります。



Q02 スマートフォンを利用する場合、こんな点に注意!

A02 注意 注意しましょう

パケット通信料が**高額**になる場合があります。
セキュリティ上の**危険性**に注意が必要です。

料金について

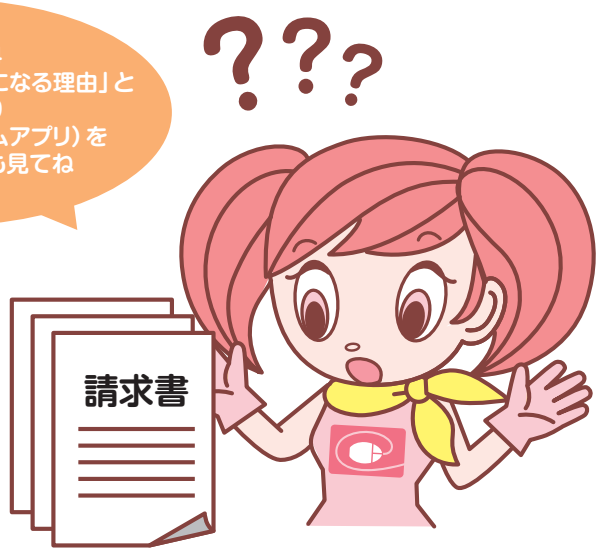
パケット通信料が高額になる場合があります。

●パソコン用のウェブサイト閲覧や動画視聴をすると大容量のデータ通信が行われます。

●また、スマートフォンは従来の携帯電話と違い、電源を入れていれば、操作しなくても自動で通信を行うことがあります。このため、従来の携帯電話に比べてパケット通信料が高額になりやすくなっています。ご自身では通信をしているつもりがなくても予期せぬパケット通信料金が発生する場合がありますので注意してください。

●パケット通信料が思いがけず高額となることを防止するには、パケット定額制を利用することも有効です。また、スマートフォンではパケット通信(データ通信)をオフにすることができるほか、パケット通信以外にWi-Fiなどの無線アクセスサービスを利用することができます。

P15のA14
「パケット通信料が高額になる理由」と
P17のA19
「ゲームサイト(ゲームアプリ)を
利用するときは」も見てね



特集

スマートフォンの便利さと注意点

セキュリティについて

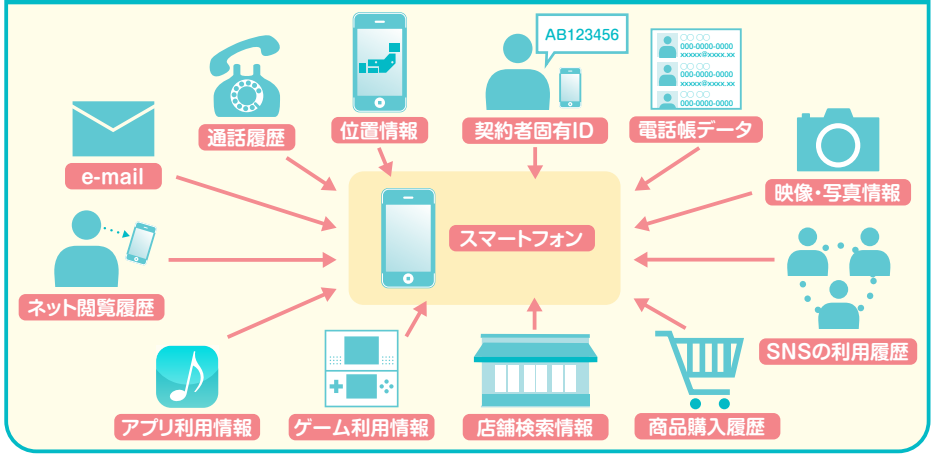
Wi-Fiなどの携帯電話会社のネットワークを介さない利用や、アプリケーションの利用の際には、セキュリティ上の危険性に注意が必要です。

●これまでの携帯電話端末と異なり、スマートフォンは、パソコンの場合と同様、ウイルスに感染するおそれがあるなど情報セキュリティ上の危険が高くなっています。
対策としては、OS（基本ソフト）の更新や、スマートフォン用のセキュリティ対策ソフトの利用を確認することや、信頼できるアプリケーション・マーケットからアプリケーションを入手することが有効です。

●スマートフォンは、これまでの携帯電話端末と比較して、多くの個人に関する情報（電話帳、位置情報など）が保存されています。そのため、普段からパスワードロックを掛けておくなど端末の紛失や盗難への対策を講じておきましょう。

●スマートフォンのアプリには、電話帳情報や位置情報等の利用者情報をアプリの機能に使用するほか、広告表示等のために取得し、外部に送信するものがあります。アプリを利用する際には、そのダウンロードや利用（起動）時等に、プライバシーポリシーやアプリの利用規約等を読み、取得される利用者情報の範囲等をよく確認したうえで同意・利用するように努めましょう。

スマートフォンにおける主な利用者情報



特集

ソーシャルメディアの利用の注意

Q 03 ソーシャルメディアを利用するにあたって気をつけなければいけないことはあるの？

A 03 基礎知識 知っておきましょう

現実社会で守るべき義務や心がけたい道徳、必要な思いやりがあるのと同様に、インターネット上におけるソーシャルメディアの利用においても、ルールやモラル、マナーを守って利用をしないと、思いがけないトラブルに巻き込まれることもあります。

ソーシャルメディアとは、インターネットを利用して誰でも手軽に情報を発信したり、相互のやりとりができる双方向のメディアです。発信した情報は、親しい人だけが見ているだけではなく、いろいろな人がその情報を入手できる可能性があります。そのため、発信者はちょっとした悪ふざけのつもりで行った行為が、ソーシャルメディアへ投稿することによって、一般の人々や社会に対して大きな影響を及ぼす事例、発信者自身及び関係者がトラブルに巻き込まれたり処罰されたりする事例も生じています。

●ソーシャルメディアを利用するにあたっては、以下のことを注意して利用しましょう。

① インターネットは世界中の人が使う公共メディアであることを意識しましょう。
② 現実社会と同様に、ルール、マナー等を守りましょう。
③ 自分はもちろん、友人・知人の個人情報に関する書き込みも行わないよう気をつけましょう。
④ 自分以外の人の写った写真や情報を発信する際は、あらかじめその人に許可を得ましょう。
⑤ 他人になりすまして情報を発信してはいけません。
⑥ 「友だち」の登録は、信頼できる“知っている人”だけにしましょう。また、知っている人から「友だち申請」が届いたとしても、本当に本人かどうかをしっかり確かめましょう。
⑦ 他人を中傷したり、侮辱したりするような投稿をしてはいけません。
⑧ ソーシャルメディア提供側が示す利用規約を必ず読み、正しく理解したうえで、利用しましょう。

安心ネットづくり促進協議会
http://www.good-net.jp/

特集

SIMロック解除、格安スマホについて

Q04 SIMロック解除ができるのはいつからなの？

A04 基礎知識 知っておきましょう

今でも一部の携帯電話については可能ですが、
平成27年5月1日以降新たに発売される携帯電話・タブレット等については、利用者からの求めがあった場合は原則としてSIMロック解除に対応することになります。

●SIMロックとは、特定のSIM（携帯電話サービス等の契約者を特定するための情報を記録したICカード）が差し込まれた場合にのみ動作するよう設定された端末上の制限のことです。SIMロック解除とは、SIMロックの設定を無効化することです。

●平成27年5月1日以降に新たに発売されるスマートフォンやタブレット等の端末について、携帯電話事業者は一定期間経過後、原則無料でSIMロック解除に応じることとなっています。これにより、端末を買い換えずに他の携帯電話事業者の通信サービスに乗り換えることが可能となります。

●SIMロック解除した端末に現在の契約先とは異なる別事業者のSIMを差した場合、今、利用している通信サービス、アプリケーション等の全部または一部が使用できない可能性があります。契約前に、十分確認したうえでご利用ください。

Q05 格安スマホとは、どのようなサービスなの？

A05 基礎知識 知っておきましょう

携帯電話事業者のネットワークを利用することにより、比較的安価な独自のサービスを提供しています。

●いわゆる格安スマホ等を提供する事業者は、自らは電波の割当てを受けず、電波を割り当てられた携帯電話事業者からネットワークを借りて独自のサービスを提供する事業者であり、そういった事業者は、MVNO（※）と呼ばれます。

※MVNO（Mobile Virtual Network Operator）：仮想移動体通信事業者

●SIMにより独自の料金プランでスマートフォン向けサービスを提供しており、大手スーパーや家電量販店等において、端末とセットで提供されるケースもあります。

●通信容量や通信速度に制限を設ける代わりに料金を抑えるなど、利用者のニーズを踏まえたさまざまな創意工夫がなされています。サービスの内容や契約条件は事業者によって異なりますので、契約の際は事業者に詳細を確認のうえ、十分に検討しましょう。

知っ得情報

勧誘や契約時の説明等に関するQ&A

Q06 電気通信サービスを利用するためには、どのような点に注意が必要なの？

A06 注意 注意しましょう

契約時には
サービス内容 **契約内容** **利用料金** **解約条件**
等を**よく確認**しましょう。

電気通信サービスの契約内容などが十分に理解されていないことから生じるトラブルを回避するため、電気通信事業者や代理店等には、契約する前に説明することが義務付けられています。一方で、利用者においても、サービスの内容、料金その他の支払いが必要になる経費、契約の解除に伴う制限や違約金の有無を積極的に確認するよう心がけましょう。

契約時の注意点

●サービスの内容、料金等を、契約締結前によく確認しましょう。また、後日、確認ができるよう、契約締結時に交付された書面をしっかりと保存しましょう。

●契約内容等、サービスの内容に不明点があった場合に確認ができるよう、契約の相手方及び問い合わせ窓口を確認するようにしましょう。

●基本料金など、一定期間の契約継続を前提に料金が割引になる場合、途中で契約を解除すると違約金が発生することがあります。また、一定期間終了後も、更新拒絶の意思表示がない場合、自動更新されることがあります。見た目の安さで判断せず、利用目的に合った料金プランを選択するよう、サービスの内容の説明を受けたり、カタログやホームページで十分に確認しましょう。また、電気通信事業者によっては、希望者に対し、契約解除期間をお知らせしている場合もあるので、電気通信事業者に相談しましょう。

●オプションサービスに加入したり、他のサービスや電子機器等とセットで加入すると携帯端末や利用料金が割引される場合は、割引条件や加入したオプション等の内容を確認しましょう。また、加入したオプションサービス等が不要となった場合は利用者自身による解約が必要となる場合があります。加入したオプションサービス等を把握するとともに、不要となった場合の解約方法についても確認しましょう。

勧誘や契約時の説明等に関するQ&A

携帯電話、モバイルデータ通信等

●携帯電話、モバイルデータ通信やWi-Fiなど無線の電気通信サービスを選ぶときは、サービスを受けることができる地域か、通信環境によってサービスの品質が低下することがあるかなどをよく確認しましょう。

●携帯電話の契約を結ぶときは、本人確認書類が必要になります。必要な書類や手続については、各電気通信事業者にお問い合わせください。

●携帯電話を海外で利用する場合の通話料・パケット通信料は、日本の料金体系とは異なり、各種割引サービスが適用されずに、高額になることがあります。特に、スマートフォンの場合は、自動でアプリケーションが通信を行うことによる、高額のパケット通信の請求が発生するおそれがあるので十分注意してください。

4ページのA02【スマートフォンを利用する場合、こんな点に注意!】もご覧ください。 P4 A02 参照

●携帯電話が第三者に使われることにより、高額請求の被害にあうケースが発生しています。盗難・紛失した場合には、速やかに契約している携帯電話会社に連絡しましょう。また、気軽なアルバイトのつもりで、携帯電話を契約して他人に渡しても、その料金や携帯電話端末の代金などは契約者に請求されます。このようなアルバイトには決して応募しないようにしましょう。

固定電話、IP電話、インターネット接続サービス

●電話サービスを選ぶときには、利用（接続）できない番号の有無をよく確認しましょう。

●電話サービスやインターネット接続サービス等を選ぶときは、サービス料金以外の工事費やモデムレンタル料の有無、サービス提供開始までの期間等をよく確認しましょう。

●インターネット接続サービスでは、契約時はプロバイダが回線事業者の契約の取次ぎをする場合がありますが、サービスを解約する場合には、プロバイダと回線事業者のそれぞれのサービスの解約手続きをしないと契約が継続されて、料金徴収が続くことになるので、注意が必要です。

●プロバイダの契約にあたり、電話で勧誘され、遠隔操作により自分のパソコンを設定させる場合は、遠隔操作によりなにが行われるのかを事前にきちんと確認し、契約内容を十分に理解したうえで契約をしましょう。また、遠隔操作により、意図していない自分のパソコンの中の情報が外部に漏れる可能性があることに注意しましょう。

未成年者の契約について

●未成年者が携帯電話やインターネット等の契約を行う場合、親権者の同意が必要となります。

●未成年者の加入契約の際に、親権者の同意を得ていない契約は取消しができる場合がありますが、未成年者が成人と偽って契約した場合等には取消しができないことがあります。

●契約の際には、親権者の同意書類が必要になります。詳しい手続き等については各電気通信事業者にお問い合わせください。

Q07 インターネット回線（光ファイバーやモバイルデータ通信）などの勧誘を受けたときは、どんな点に注意が必要なの？

A07 基礎知識 知っておきましょう　その場ですぐ契約せず、十分に検討しましょう。

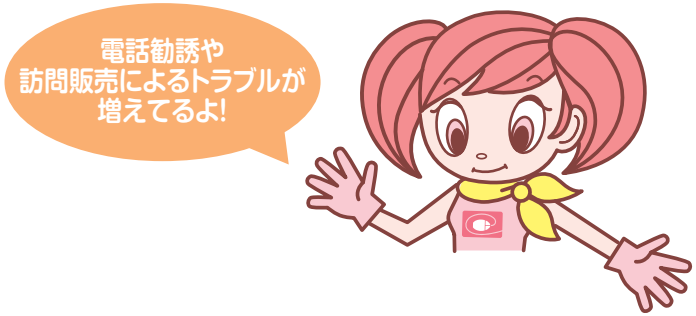
サービス内容が分からない場合、加入する必要があるかどうか分からない場合、勧誘が強引だと感じた場合には、その場ですぐ契約（申込み）したり、曖昧な返事をせずに、契約内容を確認し、十分に検討を行うようにしてください。

勧誘を受けた際の注意点

●電話勧誘や訪問販売によるトラブルが増えています。契約は口頭でも成立します。サービスの内容が分からない場合、その場ですぐ契約（申込み）せずに、分かるまで説明を聞いたり、家族に相談したりして決めるよう心がけてください。契約（申込み）する意思がない場合は、曖昧な返事をせず、はっきりと意思表示することも重要です。

●電気通信サービスにクーリングオフは適用されません。契約（申込み）を行う際は慎重に検討しましょう。どうしても不要だという場合、インターネット回線は工事前や電気通信事業者によっては一定期間内であれば解約（キャンセル）が可能な場合があります。契約先の電気通信事業者に相談してください。

●基本料金など、一定期間の契約継続を前提に料金が割引になる場合、途中で契約を解除すると違約金が発生することがあります。また、一定期間終了後も、更新拒絶の意思表示がない場合、自動更新されることがあります。見た目の安さで判断せず、利用目的に合った料金プランを選択するよう、サービス内容の説明を受けたり、カタログやホームページで十分に確認しましょう。また、電気通信事業者によっては、希望者に対し、契約解除期間をお知らせしている場合もあるので、電気通信事業者に相談しましょう。



光回線サービスの乗換えについて

●NTT東西が平成27年2月から光回線サービスの卸売を開始しました。この「卸売」の提供を受けた電気通信事業者が、電話勧誘等により光回線サービスの営業活動を行っている場合があります。このサービスは、従来の工事等を伴うサービス乗換えとは異なり、「転用」という簡易な手続きによりサービス乗換えが可能となります。サービス内容や契約条件は乗換え先の電気通信事業者により異なりますので、電気通信事業者に詳細を確認のうえ、十分に検討しましょう。

●乗換えにあたっては、特に以下の点に注意しましょう。

① サービス提供者がNTT東西から変更になります。オプションサービスの扱いは乗換え先の電気通信事業者により異なりますので、十分に確認してください。

② 現在契約しているプロバイダに対し、解約手続きが必要となる場合があります。その場合、通常は解約料（違約金）が発生します。

③ サービスの乗換えにより、メールアドレスが変更になる場合があります。

④ 一度サービスの乗換えが完了すると、元のサービスに戻す際や、別の電気通信事業者のサービスに乗り換える際には、電話番号の変更が必要となったり、解約料や工事が発生する場合があります。

電気通信消費者情報コーナー
▶ http://www.soumu.go.jp/main_sosiki/joho_tsusin/s-jyoho.html

架空請求・不当請求トラブルに関するQ&A

Q08 まったく身に覚えのない料金請求のメールが何度も届くのですが、支払う必要はあるの？

A08 注意しましょう

まったく契約した覚えがなければ、支払う義務はありません。
身に覚えのない請求のメールは**無視しましょう。**

契約しているプロバイダや携帯電話会社の迷惑メール対策サービスを利用して、迷惑請求メールをブロックすることも有効です。設定の方法については、契約しているプロバイダや携帯電話会社にご確認ください。
お子様が携帯電話やパソコンを利用してトラブルに巻き込まれた場合には、保護者の方にすぐに連絡するよう、日頃からお子様に注意しておくことが重要です。

Q09 URLをクリックしたら、いきなり「登録完了画面」になってしまいました。どうしたらいいの？

A09 注意しましょう

契約が有効に**成立しているとは限りません。**

パソコンや携帯電話に「登録されました」や「入会ありがとうございます」と表示されても、そもそも契約が有効に成立しているとは限りません。請求されても安易に支払うことはやめましょう。

Q10 業者に連絡した方がいいの？

A10 注意しましょう

あわてて業者に連絡することは、**絶対にやめましょう。**

あわてて業者へ連絡することは、氏名や電話番号などの新たな個人情報を知らせることになるので絶対にやめましょう。一般的に、インターネット上のウェブページにアクセスした場合、メールアドレスや携帯電話事業者名が相手に伝わることがあります。しかし、これらの情報だけでは、アクセスした人を特定することはできません。過度に不安になる必要はありません。

Q11 「裁判所に訴える」、「強制執行する」などと言われていますが、どうしたらいいの？

A11 注意しましょう

そうした文言に惑わされることなく、
落ち着いて対処しましょう。

「裁判」、「強制執行」、「債権回収」等の法律用語などを持ち出してくる場合がありますが、そうした文言に惑わされることなく、落ち着いて対処しましょう。
もしも、公的機関からの通知文書等が送付された場合には、その通知文書等の真偽について、すぐに無料法律相談等、最寄りの自治体の相談窓口に相談しましょう。

Q12 請求が脅迫めいています。どうしたらいいの？

A12 注意しましょう

最寄りの**警察署に相談**しましょう。

脅迫めいた請求や、常識的に考えて迷惑な時間帯に何度も執拗に連絡してくるような場合は、恐喝等の犯罪に該当する可能性があります。最寄りの警察署に相談しましょう。

Q13 パソコンに請求画面が表示され続けてしまいます。どうしたらいいの？

A13 注意しましょう

プログラム削除の方法を確認してください。

パソコンに請求画面が表示されて消えないのは、請求画面を表示させるプログラム（コンピュータウイルス）に感染しているためです。ウイルスを駆除するためには、パソコンメーカーや契約しているプロバイダ、独立行政法人情報処理推進機構（IPA）「情報セキュリティ安心相談窓口」にプログラム削除の方法を確認してください。

「情報セキュリティ安心相談窓口」
（http://www.ipa.go.jp/security/anshin/）

知っ得情報

携帯電話やスマートフォンの高額パケット請求に関する Q&A

Q14 携帯電話やスマートフォンのパケット通信料が思いがけず高額となる理由として、どのようなものがあるの？

A14 注意しましょう

携帯電話やスマートフォンのパケット通信料は、通信時間ではなくデータ量によって変わります。また、パケット通信料が一定額で収まるプラン（パケット定額制プラン）を選んだ場合も、その対象外となる通信に注意が必要です。

- 携帯電話やスマートフォンでウェブサイト閲覧や動画視聴をしたり、ウェブサイトから音楽ファイルをダウンロードしたり、電子メールを送受信する場合にはパケット通信料が発生します。次のような場合には特に注意が必要です。
  - 音楽ファイル、動画、ゲームソフト等のデータ量が大きいアプリケーション等をダウンロードする場合
  - 通常のパソコン向けのウェブページ（フルブラウザ）を閲覧する場合
  - パソコン等に携帯電話を接続してインターネット接続を行う場合
  - 海外でインターネットへ接続する場合
- スマートフォンでは、アプリケーションの利用や自動更新等により、ご自身では通信をしているつもりがなくても予期せぬパケット通信料が発生する場合があります。
- ゲームサイト等では、ゲームのコンテンツ料金は無料の場合であっても、パケット通信料は別途発生するので注意が必要です。携帯電話でゲームサイト等を利用する場合には、パケット定額サービスへの加入をお勧めします。

P17 A19 参照

17ページのA19【携帯電話の利用時に関するQ&A】もご覧ください。

Q15 パケット通信料が高額となるのを防止するためには、どのような対策が必要なの？

A15 注意しましょう

契約時にパケット通信に関する説明を受けることや、携帯電話事業者のカタログ、ホームページなどで確認することが必要です。

次のような点について、確認することが必要です。

- 利用目的にあった料金プランの選択
- パケット定額制プランの利用
- パケット定額制プランの対象外となるサービス
- パケット通信料が一定額を超えた場合に、利用者に通知されるサービスや利用が制限されるサービス
- ファイルのサイズなどを参考に、ファイルをダウンロードする場合のパケット通信料

携帯電話 スマートフォン

携帯電話利用時の注意点に関する Q&A

Q16 すべての携帯電話やスマートフォンで緊急地震速報が受信できると聞きましたが、本当なの？

A16 基礎知識 知っておきましょう

ほとんどの機種で受信できますが、機種によっては受信できないものもあります。

気象庁が発表する緊急地震速報は、テレビ・ラジオ、防災行政無線、専用受信端末のほか、携帯電話やスマートフォンでも見聞きすることができます。販売年月が古いものや一部においては対応していない機種もありますので、ご自身の端末が対応しているかどうか携帯電話会社のホームページ等で調べておきましょう。

- 通話中には受信することができません。また、機種によってはメール送受信中にも受信することができません。
- また、スマートフォンの場合、アプリケーションのダウンロードが別途必要な場合があります。受信設定の詳細はお使いの携帯電話会社にご確認ください。

Q17 災害時や通信混雑時に携帯電話を使うには、どんな点に注意が必要なの？

A17 基礎知識 知っておきましょう

緊急時以外は通話を控え、災害用伝言サービスや電子メールを利用するよう心がけましょう。

災害時などには、本当に必要な通信を確保するため、音声通話の規制を行うことがあります。緊急を要する場合以外の通話は控え、災害用伝言サービスや電子メールを利用するよう心がけましょう。

- 利用者が一斉に電話を掛けることが予想される場合、電気通信事業者では、一定時間音声通話の利用を制限することがあります。これにより、通信網のふくそうを回避し、緊急通報などの通話を可能とすることができます。
- 通話の集中があらかじめ予想される災害時や年末年始などは、電話の利用を控え、災害用伝言サービスや電子メールを利用するようにしてください。また、緊急時の連絡手段については、家庭や職場において日頃から確認を行っておくことも重要です。

P35 A43 参照

35ページのA43【災害用の伝言サービスに関するQ&A】もご覧ください。

携帯電話利用時の注意点に関するQ&A

Q18 携帯電話が故障したので修理に出したところ、水濡れが原因だと言われました。水に濡らした覚えはないのに・・・。

A18 注意しましょう　携帯電話は精密機械です。**取扱いには注意**しましょう。

携帯電話は、精密機械なので湿気に敏感です。携帯電話を胸ポケットなどに入れている場合には、汗や体温による湿気が発生することがあります。また、スマートフォンの液晶は割れやすいうえ、機能が高度化しているため、水濡れや落下等の衝撃によって故障につながるおそれがあります。取扱いには十分注意しましょう。

Q19 携帯電話やスマートフォンのゲームサイト（ゲームアプリ）を利用するためには、どのような点に注意が必要なの？

A19 注意しましょう　**料金**についてきちんと**確認**するようにしましょう。

- 携帯電話のゲームサイトやスマートフォンのゲームアプリには、ゲーム自体は「無料」であっても、ゲーム内の自分の分身を飾るアイテムやゲームを有利に進めるための特別なアイテムは、「有料」となっている場合があります。また、サイトの利用にはパケット通信料が発生します。利用の際には、これらについてきちんと確認するようにしましょう。また、未成年者が利用する際には、親権者に確認するようにしましょう。
- 有料のゲームサイトによっては、アイテム課金などの利用金額に上限を設定することが可能な場合があります。気が付かないうちに高額な利用料となることを防ぐために有効な手段です。

Q20 中古の携帯電話端末やスマートフォンを売買したいのですが、なにか注意する点はあるの？

A20 注意しましょう　一部の携帯電話事業者では、通話・通信サービスが利用できないように**制限**をかけることがあります。また、自分が携帯電話事業者と契約していて、通話することができる携帯電話端末を他人に譲渡する場合は、親族等に譲渡する場合を除いて、あらかじめ**携帯電話事業者の承諾**が必要です。

- 盗難や契約時における本人確認書類の偽造等により、不正に入手された携帯電話端末の一部が中古市場に流通している事実があります。このため、一部の携帯電話事業者では、現在の利用者としては不正な方法で入手していない携帯電話端末であっても、盗難や本人確認書類の偽造等により不正に入手された携帯電話端末であることが明らかになった場合、通話・通信サービスが利用できないように接続制限をかけることがあります。
- 携帯電話事業者などの販売店以外（ネットオークションなど）で携帯電話端末を購入する場合には、接続制限対象の端末かどうかを携帯電話会社が開設している確認サイトで確認してから購入しましょう。
- 自分が携帯電話事業者と契約し、利用している携帯電話端末を他人に譲渡する場合は、家族等に譲渡する場合を除いて、あらかじめ携帯電話事業者の承諾を得なければなりません。携帯電話事業者の承諾を得ずに、業として有償で譲渡すると処罰されます。そのような勧誘や広告行為についても、同様に処罰されますのでご注意ください。

接続制限対象の端末かどうか
確認サイトで確認しよう

Q21 迷惑メールを受信しないようにするためには どうしたらいいの?

A21 基礎知識 知っておきましょう

迷惑メールを受信しないようにするための基本の対処法

❶アドレスを安易に公表しない
❷不用意に同意（登録）しない
❸推測されにくいアドレスを使う
} を守りましょう。

また、携帯電話事業者などが提供する
迷惑メールフィルタサービスを
利用することも有効です。

●迷惑メール送信者は、さまざまな手段を講じてあなたの大切なアドレスを入手しようとしています。迷惑メールを受信しないようにするために次の基本の対処法を守り、アドレスを知られないようにしましょう。

① アドレスを安易に公表しない

あなたのアドレスをホームページ、ブログ、SNSなどインターネット上に安易に公表すると、アドレス収集ソフト等により迷惑メール送信者にアドレスを収集される危険があります。アドレスの公表には十分に注意しましょう。

② 不用意に同意（登録）しない

インターネット上には、アドレスの収集を目的とするいわゆる「おとりサイト」があります。懸賞サイト、占いサイトなど、さまざまなサービスの無償提供を装って利用登録時にアドレスを入力させる手口です。サイト運営者がよく分からないなど、少しでもサイトの利用に不安を感じた場合は、サイトの利用に同意（登録）しないようにしましょう。

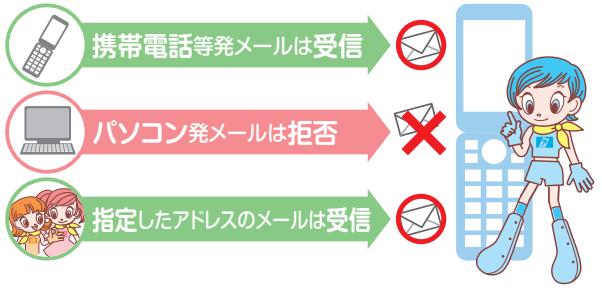
③ 推測されにくいアドレスを使う

迷惑メール送信者は、アドレスに使われそうな文字を推測してメールを送信することがあります。短くて分かりやすいアドレスは、友人に教えたりする際に楽ですが、その分迷惑メール送信者にアドレスを推測される危険が高まります。英字と数字を組み合わせ、さらに文字数も多くするなど推測されにくいアドレスを使いましょう。

指定したドメインやアドレスからのメールのみ受信するように設定する。

迷惑メール送信業者は、パソコンから大量に送信するのが通例です。そこで、携帯電話を利用している場合は、パソコン発の迷惑メールをブロックするため、携帯電話事業者のドメインから送信されるメールのみ受信するなどの「ドメイン指定受信」機能を活用することも有効な対策となります。

（なお、この場合、パソコン発のメールであっても、受信したいメールがある場合は、事前にその特定のアドレス等を受信するよう設定しておけば、受信することが可能です。）

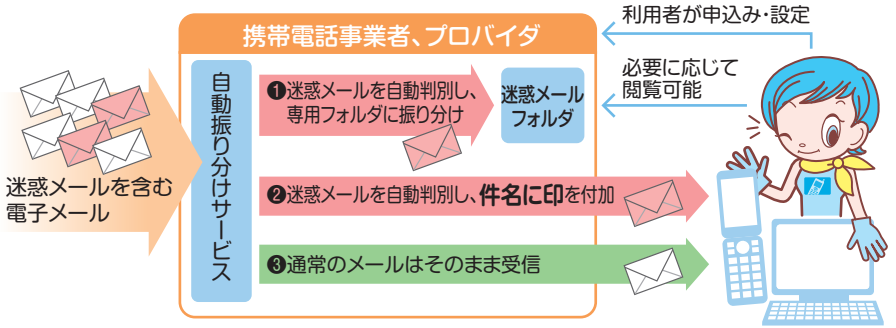


迷惑メールフィルタサービスなどを利用する。

携帯電話事業者やプロバイダでは、迷惑メールと思われる受信メールを自動的に判別して振り分けたり、件名に迷惑メールと分かる印を付けるなどのサービス（迷惑メールフィルタサービス）を提供したりしていることがあります。迷惑メールを受信しないためには、そういったサービスを利用することも有効な対策の一つです。

迷惑メールフィルタサービスは、基本的に利用する側が設定して初めて有効化するようになっています。利用している事業者の提供するサービスを確認して、自分で設定を行うことが大切です。

また、携帯電話事業者やプロバイダにより「なりすましメール対策サービス」も提供されており、このようなサービスを活用することにより、自分のメールアドレスが送信者のメールアドレスになっているメールや、知り合い、有名企業などになりすましたメールのブロックにも有効です。



Q22 身に覚えのないメールを受信してしまった場合には、どうすればいいの？

A22 基礎知識 知っておきましょう

迷惑メールを受信した場合の**基本の対処法**

1. メールを開かない
2. メールに記載されたURLをクリックしない
3. 個人情報を入力しない

を守りましょう。

●迷惑メールを受信しないように注意していても、さまざまなきっかけで、あなたのアドレスが迷惑メール送信業者に渡ってしまう可能性があります。迷惑メールフィルタを使用しても、迷惑メールがすり抜けてくることもあります。迷惑メールを受信した場合における次の基本の対処法を守り、迷惑メールからつながる第2、第3のトラブルを未然に防ぐことが大切です。

① メールを開かない

迷惑メールや迷惑メールに添付されているファイルを開いてしまうと、ウイルス感染や望まない画像などが表示されるおそれがあります。心当たりがないアドレスから送信されたメールは開かずにそのまま削除しましょう。

② メールに記載されたURLをクリックしない

迷惑メールに記載されているURL（リンク先）をクリックしないようにしましょう。安易にURLをクリックすると、サイトの運営者からサイトの閲覧料や利用料と称して不当な料金請求などを受けるきっかけになります。

③ 個人情報を入力しない

迷惑メールの中には、有名企業を装った偽サイトへ誘導し、IDやパスワードなどの個人情報の入力を要求する、いわゆる「フィッシングメール」もあります。個人情報を要求する怪しいメールを受けとった場合は、安易に個人情報を入力するのではなく、直接利用会社に問い合わせを行うなどの確認をしましょう。

迷惑メール相談センターでは、迷惑メールに関する情報提供を受け付けています。
迷惑メールを受信された場合は次のアドレスに転送してください。
転送先アドレス meiwaku@dekyo.or.jp
※携帯電話から転送する場合は、本文の文頭に「受信月日」「送信者アドレス（Fromアドレス）」を追加記載してください。

Q23 フィルタリングとは？

A23 基礎知識 知っておきましょう

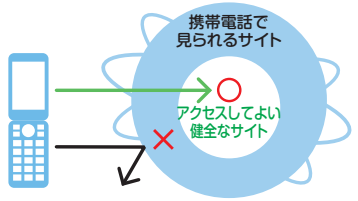
出会い系サイト、アダルトサイト等、青少年に見せたくないインターネット上の情報の**閲覧を制限**する機能のことです。

フィルタリングは、違法・有害なサイトを見ることができないようにするばかりでなく、悪質・違法なサイトにアクセスすることによって発生するトラブル（不当な高額請求、迷惑メールの受信等）からの回避効果もあるため、子どもたちをインターネットを通じたトラブルから保護する有効な手段でもあります。

フィルタリングの方式としては、**①ホワイトリスト方式、②ブラックリスト方式**があり、お子さんの成長にあわせて適切な方式を選択することが重要です。

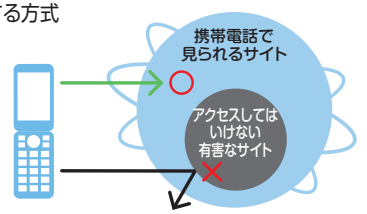
ホワイトリスト方式

子どもにとって安全で有益と思われる、**一定の基準を満たしたサイトのみにアクセス可能で**、それ以外のサイトへのアクセスを制限する方式



ブラックリスト方式

原則すべてのサイトにアクセス可能ですが、出会い系やギャンブル等、子どもに有害と思われる**特定のサイトへのアクセスだけを制限**する方式



Q24 携帯電話・スマートフォンにおけるフィルタリングの設定について、法律ではどのように規定されているの？

A24 基礎知識 知っておきましょう

携帯電話事業者は、「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」により、青少年（18歳未満の者）が利用する携帯電話・スマートフォンの契約をする場合、保護者からフィルタリングサービスを不要とする申出がない限り、フィルタリングサービスを提供することを義務付けられています（第17条1項）。

保護者についても、青少年に使用させる携帯電話の契約時に、使用者が青少年であることを携帯電話事業者に申告する義務があります（第17条2項）。保護者は店頭でフィルタリングの説明をよく聞き、フィルタリングを利用するかどうかについて、よく考えたうえで責任を持って判断をすることが大切です。

Q25 フィルタリングを利用するには、どのような方法があるの？

A25 基礎知識 知っておきましょう

携帯電話事業者が提供するフィルタリングサービスを利用したり、市販のフィルタリングソフトをインストールしたりするなどの方法があります。

従来の携帯電話では、フィルタリングは携帯電話事業者が管理する3G・LTE等のネットワーク上で提供されています。ただその場合、スマートフォンでよく利用されるアプリケーションや無線LANを通したインターネット接続についてはフィルタリングがかからない場合があります。そのため、一部の携帯電話事業者においては、**多様なアプリケーションを一定の基準に基づき起動制限する機能や、無線LAN経由のインターネット接続においてもフィルタリング機能を持つフィルタリングソフトの提供を始めています。**店頭等でよく説明を聞き、適切なフィルタリングの選択を心がけましょう。なお、携帯型ゲーム機などにはフィルタリングと同様の機能として、ペアレンタルコントロールが組み込まれています。保護者の方は利用者の年齢にあった適切な設定をしましょう。詳しくは、各機器の取扱説明書やメーカーのホームページ等をご覧ください。

フィルタリング紹介サイト

総務省「フィルタリング（有害サイトアクセス制限サービス）をご存知ですか?」
▶ http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/filtering.html

（社）電気通信事業者協会ホームページ「有害サイトアクセス制限サービス」
▶ http://www.tca.or.jp/mobile/filtering.html

携帯電話各社におけるフィルタリングサービスのお問い合わせ先〈2015年1月現在〉

docomo	【ドコモの携帯電話から】……局番なし151（無料） 【一般電話から】……0120−800−000（無料）
au	【auの携帯電話から】……局番なし157（無料） 【一般電話から】……0077−7−111（無料）
SoftBank	【ソフトバンクの携帯電話から】……局番なし157（無料） 【一般電話から】……0800−919−0157（無料）
Y!mobile	【ワイモバイルの携帯電話・PHSから】……局番なし151（通話料有料） 【一般電話から】……0570−039−151（通話料有料）

Q26 携帯電話のフィルタリングサービスを設定すると、コミュニケーション機能を持つサイトやアプリ(※)については閲覧制限の対象に含まれるため一律にアクセスできなくなり、不便であると聞きましたが、本当なの？

※ 同じ興味や関心を持つ者同士が、掲示板等を利用して情報を交換・共有することができるサイトやアプリ

A26 基礎知識 知っておきましょう

第三者機関(※)が認定したサイトやアプリについては、本来は閲覧制限に含まれていても、その健全性が認められ、携帯電話事業者が提供するフィルタリングサービスを設定していても閲覧することが可能となっています。

なお、携帯電話事業者が提供するフィルタリングサービスでは、閲覧制限の対象となっているサイトやアプリについて、保護者が閲覧可能なサイトを個別に設定できる機能（いわゆる「カスタマイズ機能」）が備わっているものもあり、この機能を利用すれば、お子さんの成長やご家庭の方針にあわせて閲覧可能な範囲を設定することができます。

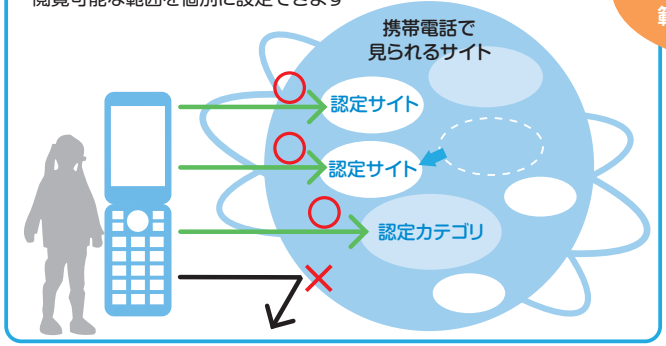
※モバイルコンテンツ審査・運用監視機構（EMA）
青少年を違法・有害情報から保護し、健全なモバイルコンテンツの発展を促進することを目的として設立された第三者機関です。現在の認定サイトについては、こちらをご覧ください。

有害サイトから子供を守る！

【PC】 http://www.ema.or.jp/ema.html
【携帯】 http://www.ema.or.jp/m/

カスタマイズ機能

閲覧可能な範囲を個別に設定できます



携帯電話とPHSの電話番号に関するQ&A

Q27 携帯電話との間で、PHSも番号ポータビリティ(※)が利用できるようになったと聞いたけど、本当なの？

A27 平成26年10月1日から、**携帯電話とPHS間でも番号ポータビリティが始まりました。**
すでに提供されている携帯電話間に加えて、携帯電話とPHS間でも番号ポータビリティが利用できるようになりました。

※番号ポータビリティとは、電話の利用者が電話会社を変更した場合に、電話番号はそのままで変更後の電話会社のサービスを利用できるサービスです。

Q28 携帯電話とPHS間の番号ポータビリティができるようになったら、070・080・090から始まる番号へ電話をかけるとき、相手が携帯電話かPHSか分からなくならないの？

A28 PHSに電話をかけると、通常の呼出し音の前に「ププープー、ププープー」という識別音が鳴るため、相手がPHSであることが分かるようになっています。

なお、平成26年10月1日までは、「070-5または6で始まる番号はPHS」というように、電話番号から携帯電話とPHSを区別することができましたが、携帯電話とPHS間の番号ポータビリティ開始により、電話番号からは携帯電話とPHSを区別することができなくなりました。

Q29 固定電話から携帯電話にかける時、選択中継サービス(※)を利用しているけど、PHSにかける時でも利用できるの？

A29 PHSにかける場合でも、**選択中継サービスを利用できます。**

携帯電話とPHS間の番号ポータビリティの開始にあわせて、PHS宛ての電話についても選択中継サービスを利用できるようになりました。電話機や構内交換機の設定方法については、機器のマニュアルをご覧いただくか、ご利用の選択中継事業者や保守管理業者にご相談ください。

※選択中継サービスとは、固定電話から携帯電話またはPHSに電話をかけるときに、事業者識別番号（00XY）を相手先電話番号の前につけることにより中継事業者を選択し、割安な料金で通話ができるサービスです。

携帯電話・PHSの番号ポータビリティに関するQ&A

Q30 携帯電話とPHS間でSMS（ショートメッセージサービス）は送受信できるの？

A30 はい、携帯電話とPHS間で**SMS送受信ができます。**

携帯電話とPHS間の番号ポータビリティの開始にあわせて、携帯電話とPHS間でのSMS送受信ができるようになっています。ご利用の際は、PHS端末が携帯電話とのSMS送受信に対応している必要があります。詳しくはPHS事業者にお尋ねください。

Q31 番号ポータビリティ利用の際に注意することはあるの？

A31 注意しましょう
番号ポータビリティを実施すると、変更前の電話会社との契約は解除（解約）となり、変更後の電話会社と新たに契約（新規契約）することとなります。

具体的には、以下のような点に注意が必要です。

❶衛星船舶電話サービス及び衛星携帯電話サービス、データ通信専用サービス、新規契約の受付を停止している場合などは、携帯電話・PHSの番号ポータビリティが利用できない場合があります。
❷現在契約している携帯電話・PHS会社が発行したメールアドレスは引継ぎできません。
❸現在契約している携帯電話・PHS会社が提供しているサービス（料金プラン・割引サービス等）は解約とともに終了となります。
❹コンテンツプロバイダが提供しているコンテンツや電子マネー等は引継ぎできない場合があります。
❺年間契約等の割引サービスを契約している場合は、解約に伴い、別途費用が発生する場合があります。
❻変更後の携帯電話・PHS会社に対応している携帯電話・PHS端末が必要になります。
❼番号ポータビリティによって携帯電話・PHS会社を変更した場合、固定電話から携帯電話・PHSへの通話料金が変わる場合があります。

詳しくは、総務省ホームページの
「携帯電話・PHSの番号ポータビリティ」をご覧ください。
▶ http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/tel_number/mnp.html

携帯電話不正利用防止法に関するQ&A

Q32 携帯電話不正利用防止法とは、どのような法律なの？

A32 基礎知識 知っておきましょう

携帯電話を契約するときの本人確認の義務付けや、携帯電話やSIMを無断で譲渡することを禁止する法律です。

携帯電話不正利用防止法（※1）は、携帯電話事業者（※2）及び携帯電話のレンタル業者に対して契約時・譲渡時の本人確認等を義務付けるとともに、携帯電話の無断譲渡の禁止等を内容としています。携帯電話の契約をする際には店頭で本人確認を求められます（※3）。

※1 正式には「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」といいます。

※2 PHS事業者も含みます。　※3 データ通信専用端末の場合を除きます。

携帯電話不正利用防止法の主な内容

- 携帯電話事業者は、契約時・譲渡時に契約者及び譲受人の本人確認を行わなければなりません。
- 自己名義の携帯電話等を携帯電話事業者に無断で譲渡してはいけません。
- 他人名義の携帯電話等を譲渡したり、譲り受けたりしてはいけません。
- 携帯電話のレンタル業を営む場合は、契約者の本人確認を行わなければなりません。
- 携帯電話等が犯罪に利用されている場合、警察からの求めに応じて携帯電話事業者は契約者の確認を行うことができます。
- 携帯電話業者は、契約者が確認に応じない場合には役務の提供を拒むことができます。

Q33 携帯電話を契約する際、または借りる際の本人確認はどのように行うの？

A33 注意 注意しましょう

免許証やパスポート等、顔写真付きの公的身分証の提示が求められます。

本人確認の際は、原則として免許証、パスポートといった顔写真付きの公的身分証の提示を求められることになります。具体的には、各携帯電話事業者にお問い合わせください。

総務省 携帯電話不正利用防止法のページ
▶ http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.html

インターネット上の違法・有害情報に関するQ&A

Q34 インターネット上で違法・有害情報を発見した場合には、どうしたらいいの？

A34 **「インターネット・ホットラインセンター」か、警察に通報してください。**

インターネット上で違法な情報を発見した場合には、「インターネット・ホットラインセンター」か、警察に通報してください。公序良俗に反するような有害情報を見つけた場合には、「インターネット・ホットラインセンター」へ情報提供してください。なお、違法・有害情報が掲載されているサーバや電子掲示板の管理者に情報提供する方法も考えられます。

- 例えば、児童ポルノやいわゆる危険ドラッグの広告などは違法な情報とされています。
- インターネット・ホットラインセンターは、インターネット利用者から違法・有害情報に関する情報提供を受け付け、一定の基準に従って情報を選別したうえで、警察への情報提供、電子掲示板の管理者等への送信防止措置依頼等を行う民間団体です。詳しくは、ホームページをご覧ください。

インターネット・ホットラインセンター
▶ http://www.internethotline.jp/

- なお、サーバや電子掲示板の管理者が誰か分からないときは、.jpドメインの場合には（株）日本レジストリサービス、.comや.netドメインの場合には国際組織INTERNICの提供するWhoisサービスを利用することで、連絡先を調べることができます。

（株）日本レジストリサービス Whois
▶ http://whois.jprs.jp/

INTERNIC Whois
▶ http://www.internic.net/whois.html

Q35 インターネット上で自分の権利を侵害するような書き込みを発見した場合には、どうしたらいいの？

A35 **本人からサイトの管理者等に対して削除の要求をすることが可能です。**

ご自身の権利を侵害するような書き込みがあった場合には、プロバイダ責任制限法（※）や名誉棄損・プライバシー関係ガイドライン等に基づき、本人からサイトの管理者等に対して削除の要求をすることが可能です。また、サイト管理者等への削除要求の方法等について「違法・有害情報相談センター」において相談を受け付けています。

※「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」

具体的な手続き等については、こちらをご覧ください。

プロバイダ責任制限法 関連情報webサイト
▶ http://www.isplaw.jp/

違法・有害情報相談センター
▶ http://www.ihaho.jp/

インターネット上の違法・有害情報に関するQ&A

Q36 私事性的画像記録の提供等による被害の防止に関する法律とは、どのような法律なの?

A36 注意しましょう

いわゆるリベンジポルノ画像がインターネット上に流通することによって、被害者に多大な精神的被害が発生することを防止するための法律です。

私事性的画像記録の提供等による被害の防止に関する法律の主な内容

- 平成26年11月27日制定（第3条は同年12月17日、第4条は同年12月27日施行。）。
- リベンジポルノ画像を不特定または多数の人に提供すると罰せられます。
- リベンジポルノ画像によってプライバシー等を侵害された場合、プロバイダ責任制限法の特例（※）による削除の申出ができます。

※リベンジポルノ画像によってプライバシー等を侵害された人からプロバイダ等に削除の申出があった場合、プロバイダ等から発信者に対する削除同意期間が通常の「7日」から「2日」に短縮されています。

Q37 なりすましECサイトってなに?

A37 注意しましょう

実在するサイトの外観を模倣し、あたかも当該サイトであるかのように消費者を誤認させ、商品代金をだましとったり、まったく別の物を送りつけるサイトです。

実在する通販サイトを模倣したり、連絡先等を偽った通販サイトで商品を注文し、注文したものと異なる模倣品が届いたり、商品が届かず返金もされないという〝なりすましECサイト〟によるトラブルが多発しています。こうしたトラブルを避けるため、購入前には注意しましょう。

消費者庁
▶ http://www.cb-ccj.caa.go.jp/narisumashi/index.html

なりすましECサイト対策協議会
▶ http://www.saferinternet.or.jp/narisumashi/

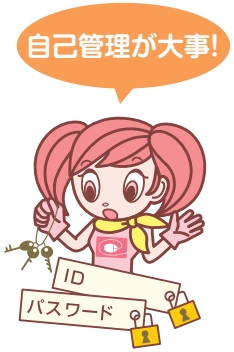
フィッシング詐欺に関するQ&A

Q38 フィッシングってなに?

A38 注意しましょう

金融機関等を装い、銀行口座番号、クレジットカード番号、暗証番号、IDやパスワードといった個人に関する情報を巧みに詐取する行為です。

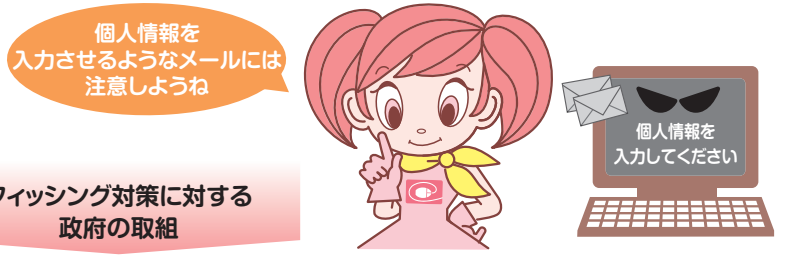
フィッシング（Phishing）とは、クレジットカード会社や銀行、オンラインショッピング事業者、オークション事業者などを装った電子メールを不特定多数に送り、偽のホームページにアクセスするよう仕向け、銀行口座番号、クレジットカード番号、暗証番号、IDやパスワードといった個人に関する情報を巧みに詐取する行為です。



金融機関等が個人に関する情報をメールで尋ねるようなことはほとんどありませんが、もし、個人に関する情報を入力させるようなメールを受信した場合は、メール本文にあるリンクはクリックせずに、金融機関等の正規のホームページを確認するなど十分注意して対応してください。

また、近年、フィッシングの手口は多様化しています。偽のメールを送る、偽のホームページに誘導するだけではなく、端末をウイルスに感染させて、利用者は正規のホームページを見ているにもかかわらず、同時に不正なポップアップ画面を出して、個人情報の入力を求める手口も出現しています。

オンライン上で個人情報を入力する際に、通常の操作手順と異なる手続きを求められた場合には、サービス提供元に確認するなど、慎重な対応をしてください。



フィッシング対策に対する政府の取組

警察庁「フィッシング110番」
▶ http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

フィッシング対策協議会
▶ http://www.antiphishing.jp

Q39 コンピュータウイルスへの感染といった、インターネット上の危険からコンピュータを守るためには、どのような対策をすればいいの？

A39 基礎知識 知っておきましょう 基本となる情報セキュリティ対策には、主に以下のものがあります。

❶ 不審なサイトへのアクセスやプログラムの実行に注意する

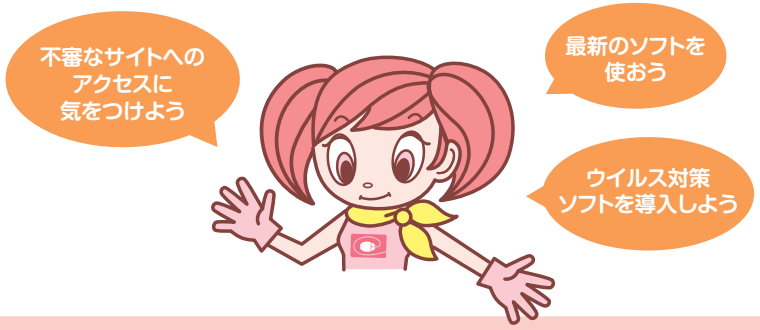
インターネット上には、有益な情報や便利なプログラムを装って利用者にサイトへのアクセスやプログラムの実行を促し、コンピュータウイルスに感染させようとするコンテンツが多くあります。インターネットを利用するにあたっては、アクセスしようとするURLや実行しようとするファイルの拡張子などに注意（例えば動画ファイルを装いながら、拡張子が.exeになっているもの　など）し、不審なものについては実行しないようにしましょう。また、短縮URLなどにより、実際にアクセスするURLとは異なるURLを表示することもできるため、URLだけで不審なサイトかどうか判断することが難しい場合があり、より注意が必要です。

❷ ソフトウェアの更新（最新のセキュリティパッチの適用）

Webブラウザや電子メールソフト、OS等のソフトウェアについて、メーカーから情報セキュリティ上の問題を解決するための修正プログラムが提供されることがあります。これらの修正プログラムを定期的に適用して、できる限りソフトウェアを最新の状態に保つように心がける必要があります。

❸ ウイルス対策サービス・ソフトの導入

最近のコンピュータウイルスは、不正なプログラムの実行やウイルスを配布するURLへのアクセスを通じて感染するものばかりではなく、ホームページを閲覧しただけで感染するものも出現してきています。ウイルスに感染しないようにするためには、ウイルス対策サービス・ソフトを導入することが有効です。



Q40 スマートフォンにも情報セキュリティ対策が必要だと聞きました。本当なの？

A40 基礎知識 知っておきましょう 利用者自身が情報セキュリティ対策を取ることが必要です。

スマートフォンは、これまでの携帯電話端末と違い、アプリケーションを通じて個人に関する情報の流出などのおそれがあります。利用者自身が情報セキュリティ対策を取ることが必要です。

スマートフォン情報セキュリティ 3か条

❶スマートフォンは、OSの更新（アップデート）が必要です。

古いOSを使っていると、ウイルス感染の危険性が高くなるので、更新の通知が来たら、速やかにインストールしましょう。

❷各電気通信事業者やセキュリティソフト提供会社では、スマートフォン向けのセキュリティ対策サービスを提供しています。

※サービスには有償のものもあります。また、ウイルス定義ファイルのアップデートのためにパケット通信料が必要な場合があります。

❸信頼できるアプリケーション・マーケットからアプリケーションを入手するようにしましょう。また、インストールする際には、アプリケーションの機能や利用条件に注意しましょう。

インターネットを利用する際の情報セキュリティ対策については、このほかにも利用の際の心構えなど、ご留意いただきたい事項があります。これらについては、以下のサイトをご覧ください。

総務省「国民のための情報セキュリティサイト」
▶ http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

インターネット上のマナーに関するQ&A

Q41 チェーンメールが送られてきました。同じ内容のメールを他人にも送るように書いてありますが、どうしたらいいの？

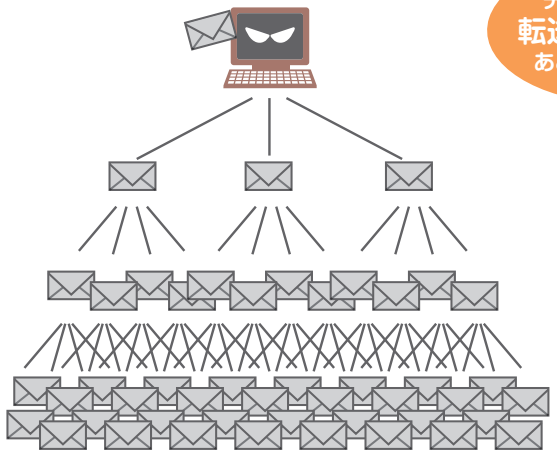
A41 基礎知識 知っておきましょう

チェーンメールは受信しても転送せずに削除し、後は気にしないようにしましょう。

チェーンメールとは、一般的に同じ内容を不特定多数の人に転送するように求める迷惑メールのことです。転送されることを目的としているため、「転送すると幸せになる」、「転送しないと不幸になる」等、さまざまな内容で転送させようとします。しかし、チェーンメールは人の心につけ込み、勝手に転送を押しつけるメールであり、貴方の周囲に悪影響を及ぼすことにもなりかねませんので、絶対に転送してはいけません。チェーンメールは受信しても転送せずに削除し、後は気にしないようにしましょう。

また、どうしても不安になり、無視できないときには、次のサイトにチェーンメール転送用アドレスが書かれていますので、そちらに転送してください。

迷惑メール相談センター「チェーンメールの転送先」
▶ http://www.dekyo.or.jp/soudan/chain/tensou.html



災害時・停電時の電話サービスの利用に関するQ&A

Q42 災害や停電が起きたとき、どんな点に注意して電話サービスを利用すればいいの？

A42 基礎知識 知っておきましょう

災害発生時は、音声通話の規制を行うことがあります。また、停電時は電源を使用する固定電話が使えなくなります。

災害発生時は、災害救助機関などに必要な通信を確保するため、音声通話の規制を行うことがあります。また、停電時は電源を使用する固定電話が使えなくなります。不要不急な通話は避け、災害用伝言版や電子メールを利用するよう心がけましょう。

- IP電話（※）には、警察や消防機関等への緊急通報（110番、119番等）が利用できないもの（050番号で始まる電話の場合）があります。
- 停電時は、電源を使用する固定電話やIP電話、ひかり電話などは基本的に使えなくなりますが、停電対応の電話機を使用されていたり、利用者で独自の電源を用意されたりしている場合には使えることもあります。なお、停電時においても公衆電話は通話可能です。
- 災害発生時は、災害救助機関などに必要な通信を確保するため、電気通信事業者では、一定時間音声通話の規制を行うことがあります。これにより、通信網の障害を回避し、緊急通報などの通話を可能とすることができます。
- 電話が大変混み合うため、不要不急な通話は控え、災害用伝言ダイヤルや災害用伝言板などのサービスや電子メールを利用するよう心がけましょう。また、緊急時の連絡手段については、家庭や職場において日頃から確認を行っておくことも重要です。

※IP（Internet Protocol）技術を利用した音声電話サービスのことで、次の2種類があります。

①0AB～J型IP電話：アナログ電話と同様の電話番号を用い、高品質な通話や緊急通報の利用が可能です。

②050型IP電話：050で始まる電話番号を用い、低料金での通話が可能ですが、緊急通報が利用できず、アナログ電話に比べ通話品質が低い場合もあります。

災害用伝言サービス

Q43 「災害用伝言ダイヤル（171）」「災害用伝言板」「災害用伝言板（web171）」 とは、どんなサービスなの？

A43 基礎知識 知っておきましょう

災害時に電話がつながりにくい状況であっても、家族や知人の間で安否確認や避難場所の連絡等を行えるサービスです。

地震や大雨・洪水などの大規模災害が発生すると、大量の電話が被災地に集中するため電話がつながりにくくなることがあります。このような場合でも、家族や知人との間での安否確認や避難場所の連絡等を行えるよう電気通信事業者が提供しているサービスです。

※ 災害が発生した際に、開設されるサービスです（ただし、体験利用できる期間があります）。

災害用伝言ダイヤル（171）の利用方法

① 171をダイヤルします。
② ガイダンスに従って、録音の場合は「1」を、再生の場合は「2」をダイヤルします。（録音・再生には暗証番号を付けられます）
③ ガイダンスに従って、自宅（被災地）の電話番号、または、連絡をとりたい被災地の方の電話番号を市外局番からダイヤルします。
④ 伝言を録音・再生することができます。

〈注意点〉
- 伝言の録音・再生は、被災地の方の電話番号宛に行う必要があり、この電話番号は03等の市外局番で始まる電話番号のみが対象です。
- 携帯電話（090、080）・PHS（070）からは、災害用伝言ダイヤルを利用することはできますが、携帯電話・PHSの電話番号宛に伝言を録音することはできませんのでご注意ください。
- 伝言録音時間は、1伝言あたり30秒以内です。
- 1電話番号あたり、10伝言まで登録できます。

災害用伝言板の利用方法

伝言の登録方法

❶ お使いの端末の携帯電話・PHS会社の災害用伝言板にアクセスします。または、一部のスマートフォンにおいては、災害用アプリケーションからアクセスします。（災害時はiモード、EZweb、Yahoo!ケータイ!、EMnet、CLUB AIR-EDGEのトップ画面に災害用伝言板の案内が表示されます。体験利用の際はメニューリスト内からアクセスしてください）
❷ 「災害用伝言板」の中の「登録」を選択します。（登録は被災地域内の携帯電話・PHSからのアクセスのみが可能です）
❸ 現在の状態について「無事です」等の選択肢から選び、任意で100文字以内のコメントを入力します。（状態の複数選択や、コメントのみの利用も可能です）
❹ 最後に「登録」を押して、伝言板への登録が完了となります。

伝言の確認方法

❶ お使いの端末の携帯電話・PHS会社の災害用伝言板にアクセスします。（伝言の確認はPC等からも行うことができます）
❷ 「災害用伝言板」の中の「確認」を選択します。（確認は全国からのアクセスが可能です）
❸ 安否を確認したい方の携帯電話・PHS番号を入力し「検索」を押します。
❹ 伝言一覧が表示されますので、詳細を確認したい伝言を選択してください。

〈注意点〉
- 1電話番号あたり、最大10伝言まで登録できます。
- 伝言の保存期間は、1つの災害での災害用伝言板を終了するまでです。
- 災害用伝言板の利用料・パケット通信料は無料です。
- 携帯電話・PHS会社の災害用伝言板及びNTT東西の災害用伝言板（web171）を横断して検索できます。

災害用伝言板（web171）の利用方法

❶ https://www.web171.jp/へアクセスします。
❷ 連絡をとりたい方の固定電話番号や携帯電話番号を入力します。
❸ 伝言を登録・確認することができます。（事前に設定することで閲覧者を限定することもできます）

〈注意点〉
- 1電話番号あたり、20伝言まで蓄積できます。
- 文字（テキスト）1伝言あたり全角100文字まで

そのほか、携帯電話・PHS各社は、音声をパケット通信で送信する「災害用音声お届けサービス」の提供や、スマートフォン用に災害アプリケーション等を用意しております。詳しくは電気通信事業者のホームページをご覧ください。

Q44 ユニバーサルサービス（基礎的電気通信役務）とはどんなサービスなの？

A44 電気通信事業法により、「国民生活に不可欠であるため日本全国で提供が確保されるべき」と規定されているサービスです。

加入電話（同程度の光IP電話を含む）の基本料や、社会生活上の安全及び戸外での最低限の通信手段を確保する観点から設置されている第一種公衆電話、さらに特例料金が設定されている離島との通話及び緊急通報（110番、118番、119番）がこれにあたります。なお、これらのユニバーサルサービスについて、現在、NTT東日本・西日本が日本全国で提供することを法令上義務付けられています。

Q45 ユニバーサルサービス料金を支払うのはなぜ？

A45 ユニバーサルサービスの日本全国での提供の維持に必要な費用が不足しているからです。

携帯電話やIP電話の普及及び電話サービスの競争の進展等で、ユニバーサルサービスの確保に必要な費用が不足しています。そのような状況の中、NTT東日本・西日本だけでユニバーサルサービスを維持することは難しいため、NTT東日本・西日本のユニバーサルサービス提供設備を利用している固定電話、携帯電話、IP電話等の電話会社もその費用を応分に負担し、全体で支えています。

多くの電話会社では、ユニバーサルサービス料金として、利用者にもご負担をお願いしています。

総務省「電話のユニバーサルサービス制度」
▶ http://www.soumu.go.jp/main_sosiki/joho_tsusin/universalservice/

(一社)電気通信事業者協会「ユニバーサルサービス支援業務」
▶ http://www.tca.or.jp/universalservice/

「加入電話」「公衆電話」「緊急通報（110番、118番、119番）」を全国どこでも公平に利用できるようみんなで支える仕組みになっています。

主な相談窓口等一覧

コンピュータウイルス等の削除方法の相談窓口

情報セキュリティ安心相談窓口
▶ http://www.ipa.go.jp/security/anshin/

P14参照

迷惑メール、チェーンメール等に関する情報提供、相談窓口

迷惑メール相談センター
▶ http://www.dekyo.or.jp/soudan/index.html

P21, P33参照

フィルタリングサービスに関する携帯電話各社のお問い合わせ先

NTTドコモ	【ドコモの携帯電話から】……局番なし151（無料） 【一般電話から】……0120−800−000（無料）
au	【auの携帯電話から】……局番なし157（無料） 【一般電話から】……0077−7−111（無料）
ソフトバンクモバイル	【ソフトバンクの携帯電話から】……局番なし157（無料） 【一般電話から】……0800−919−0157（無料）
ワイモバイル	【ワイモバイルの携帯電話・PHSから】……局番なし151（通話料有料） 【一般電話から】……0570−039−151（通話料有料）

P23参照

インターネット上の違法・有害情報に関する通報窓口

インターネット・ホットラインセンター
▶ http://www.internethotline.jp/

P28参照

インターネット上の権利侵害情報等の削除要求方法等の相談窓口

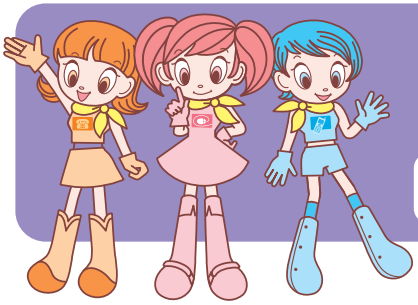
違法・有害情報相談センター
▶ http://www.ihaho.jp/

P28参照

フィッシングに関する情報提供窓口

警察庁「フィッシング110番」
▶ http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

P30参照



このハンドブックでも解決しないときは、お近くの総合通信局、または総務省電気通信消費者相談センターへ!!

ご相談はお電話で受け付けています。
受付時間／平日9:30～12:00、13:00～17:00

北海道地区にお住まいの方
総務省 北海道総合通信局
〒060-8795
札幌市北区北8条西2-1-1 札幌第1合同庁舎
電話番号 011-709-3956

信越地区にお住まいの方
総務省 信越総合通信局
〒380-8795
長野市旭町1108 長野第1合同庁舎
電話番号 026-234-9952

北陸地区にお住まいの方
総務省 北陸総合通信局
〒920-8795
金沢市広坂2-2-60 金沢広坂合同庁舎
電話番号 076-233-4429

東北地区にお住まいの方
総務省 東北総合通信局
〒980-8795
仙台市青葉区本町3-2-23 仙台第2合同庁舎
電話番号 022-221-0632

中国地区にお住まいの方
総務省 中国総合通信局
〒730-8795
広島市中区東白島町19-36
電話番号 082-222-3376

関東地区にお住まいの方
総務省 関東総合通信局
〒100-8795
千代田区九段南1-2-1 九段第3合同庁舎
電話番号 03-6238-1935

東海地区にお住まいの方
総務省 東海総合通信局
〒461-8795 名古屋市東区白壁1-15-1
名古屋合同庁舎第3号館
電話番号 052-971-9133

近畿地区にお住まいの方
総務省 近畿総合通信局
〒540-8795 大阪市中央区大手前1-5-44
大阪合同庁舎第1号館
電話番号 06-6942-8519

四国地区にお住まいの方
総務省 四国総合通信局
〒790-8795
松山市宮田町8-5
電話番号 089-936-5042

九州地区にお住まいの方
総務省 九州総合通信局
〒860-8795
熊本市西区春日2-10-1
電話番号 096-326-7862

沖縄地区にお住まいの方
総務省 沖縄総合通信事務所
〒900-8795
那覇市旭町1-9 カフーナ旭橋 B-1街区5F
電話番号 098-865-2302

総務省 電気通信消費者相談センター
〒100-8926
千代田区霞が関2-1-2 中央合同庁舎第2号館
電話番号 03-5253-5900